Data Sheet

Cisco AMP Threat Grid - Appliances

To combat malware and advanced threats, you need the best security tools available. The Cisco® Advanced Malware Protection (AMP) Threat Grid appliances combine two of the leading malware protection solutions: unified malware analysis and context-rich intelligence. They empower security professionals to proactively defend against and quickly recover from cyberattacks.

Product Overview

An AMP Threat Grid appliance delivers on-premises advanced malware analysis with deep threat analytics and content. It empowers organizations with compliance and policy restrictions by allowing them to submit malware samples to the appliance. A one-way continuous stream of federated data from AMP Threat Grid provides the malware protection you need while helping to ensure adherence to organizational requirements.

With an AMP Threat Grid appliance you can analyze all samples using proprietary and highly secure static and dynamic analysis techniques. It correlates the results with hundreds of millions of other analyzed malware artifacts to provide a global view of malware attacks, campaigns, and their distribution. Security teams can quickly correlate a single sample of observed activity and characteristics against millions of other samples to fully understand its behaviors in a historical and global context. This ability helps you effectively defend against both targeted attacks and threats from advanced malware. AMP Threat Grid's detailed reports, including the identification of important behavioral indicators and the assignment of threat scores, let you quickly prioritize and recover from advanced attacks.

Features and Benefits

AMP Threat Grid appliance features and benefits are shown in Table 1.

Table 1. Cisco AMP Threat Grid Appliance Features and Benefits

Feature	Benefit
On-premises appliance	Provides safe and highly secure on-premises static and dynamic malware analysis. Easily integrates with existing security infrastructure. Provides safe on-premises storage of malware analysis results.
Advanced analytics	Delivers comprehensive security insight into malware behavior and direct links to the sample source and associated behavior in AMP Threat Grid's extensive database. Provides easy access to all information and analysis results for further investigation.
Advanced behavioral indicators	Analyzes more than 350 highly accurate and actionable advanced behavioral indicators with low false positives. Produces comprehensive indicators through advanced static and dynamic analysis encompassing numerous malware families and malicious behaviors. Delivers the broadest context around threats and helps enable quick and confident decisions.
Threat score	Automatically derives threat scores from proprietary analysis and algorithms that consider the confidence and severity of observed actions, historical data, frequency, and clustering indicators and samples. Prioritizes threats with confidence to reflect each sample's level of malicious behavior. Improves the prioritization of threats, which enhances the efficiency and accuracy of malware analysts, incident responders, security engineering teams, and products that consume AMP Threat Grid's feeds.
API for Integration	Simplifies fast operationalization of threat intelligence with existing security and network infrastructure. Makes integration fast and easy with AMP Threat Grid's representational state transfer (REST) API. Provides integration guides for a number of third-party products, including gateways, proxies, and security information and event management (SIEM) platforms.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Comprehensive On-Premises Malware Analysis

For organizations with compliance and policy restrictions on submitting malware samples to the cloud, AMP Threat Grid provides a dedicated appliance for local malware analysis backed by the full power of AMP Threat Grid's federated threat intelligence. AMP Threat Grid provides a global view of malware attacks, campaigns, and their distribution. It analyzes millions of samples monthly and distills terabytes of malware analysis into rich, actionable intelligence.

Security teams can quickly correlate a single malware sample's observed activity and characteristics against millions of other samples to fully understand its behaviors in a historical and global context to effectively defend against both targeted attacks and the broader threats from advanced malware. AMP Threat Grid's detailed reports, identifying key behavioral indicators along with a threat score, help enable quick prioritization and recovery from advanced attacks with accuracy and speed. Analysis features include:

- Dynamic and static analysis engines that provide a full understanding of malware behavior
- Detailed analysis reports of all malware sample activities, including network traffic
- User-interface workflows designed for security operations center (SOC) analysts, malware analysts, and forensic investigators

Licensing

The Cisco AMP Threat Grid appliance licensing is based on the maximum number of files analyzed per day, as shown in Table 2.

Table 2. Cisco AMP Threat Grid Appliance Models and Licensing

	Cisco AMP Threat Grid 5000	Cisco AMP Threat Grid 5500
Maximum number of files analyzed per day	1500	5000

Product Specifications

Product specifications are shown in Table 3.

Table 3. Cisco AMP Threat Grid Appliance Produce Specifications

Feature	Cisco AMP Threat Grid 5000	Cisco AMP Threat Grid 5500
Form factor	1 rack unit (1RU)	1RU
Network interfaces	10 GB dual copper	10 GB dual copper
Power options	AC or DC	AC or DC

Ordering Information

To place an order for a Cisco AMP Threat Grid appliance, visit the Cisco ordering homepage. Table 4 provides ordering information.

Table 4. Cisco AMP Threat Grid Appliance Ordering Information

Part Number	Product Description
Cisco AMP Threat Grid 5000 Appliance and Subscription	
TG5000-BUN	Cisco AMP Threat Grid 5000 Appliance and Subscription Bundle
TG5000-K9	Cisco AMP Threat Grid 5000 Appliance with Software

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Part Number	Product Description
L-TG5000-1Y-K9	Threat Grid Content Subscription License for 5000 Model, 1 Year
L-TG5000-3Y-K9	Threat Grid Content Subscription License for 5000 Model, 3 Year
Cisco AMP Threat Grid 5500 Appliance and Subscription	
TG5500-BUN	Cisco AMP Threat Grid 5500 Appliance and Software Bundle
TG5500-K9	Cisco AMP Threat Grid 5500 Appliance with Software
L-TG5500-1Y-K9	Threat Grid Content Subscription License for 5500 Model, 1 Year
L-TG5500-3Y-K9	Threat Grid Content Subscription License for 5000 Model, 3 Year

Cisco and Partner Services

Services from Cisco and Cisco Certified Partners can help you plan and implement your integration with AMP Threat Grid’s premium threat feeds and the REST API. Planning and design services align your existing infrastructure, AMP Threat Grid premium feed formats, and operational processes to make the best use of advanced threat feeds.

Next Steps

For more information about Cisco AMP Threat Grid unified malware analysis and threat analytics, visit http://www.cisco.com/c/en/us/solutions/enterprise-networks/advanced-malware-protection/index.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C78-733667-00 01/15

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.